HACKER JOURNAL

Anno 2 - N. 35
9 Ottobre - 23 Ottobre 2003

Boss: theguilty@hackerjournal.it
Editor: grand@hackerjournal.it
Contributors: Bismark.it, DaMe`, Nicola D'Agostino, Roberto "decOder" Enea, S.O.S. - Korn, >>--Robin-->, Roberto Valloggia
DTP: Cesare Salgaro
Graphic designer: Dopla Graphic S.r.l. info@dopla.com
Copertina: Zocdesign.com
Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35
Printing
Stige (Torino)
Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.
Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. a Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile - Editore Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.
redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

BREVETTI SUL SOFTWARE:

VINTA UNA BATTAGLIA, MA LA GUERRA CONTINUA

La normativa europea sui brevetti è stata approvata, ma con modifiche sostanziali rispetto al testo proposto su "ispirazione" della BSA, l'associazione che raccoglie le principali software house mondiali. Come spesso accade dopo le elezioni, ogni parte politica in causa dichiara di aver ottenuto una importante vittoria. Possibile? Ma è proprio vero? Facciamo un passo indietro per capire innanzi tutto qual è l'oggetto del contendere.

Attualmente, in Europa la proprietà intellettuale sul software è coperta dalla legge sul diritto d'autore, e non dai brevetti. Il software è quindi paragonato più a un'opera letteraria o musicale che a un'invenzione. Non si possono brevettare le idee, ma solo la loro realizzazione pratica (le invenzioni, appunto). Anche su questo ci sarebbe da discutere, ma prendiamolo come dato di fatto. La legge votata il 22 settembre voleva appunto modificare questo stato di cose, permettendo la brevettabilità di algoritmi, porzioni di codice e semplici idee.

Su questo punto, la pressione esercitata sul parlamento europeo dalla mobilitazione di migliaia di cittadini (ma anche, bisogna dirlo, di decine di scienziati e rappresentanti di federazioni commerciali e industriali), sembra aver raggiunto i suoi scopi: per ora, il Parlamento Europeo ha stabilito che i brevetti non si possono applicare al software né alle idee.

Già, per ora, perché un testo approvato dal Parlamento Europeo non diventa automaticamente una legge valida in tutto il Vecchio Continente. La decisione finale spetta infatti alla Commissione, che non è eletta dai cittadini ma nominata dai governi. La commissione "dovrebbe" rispettare il volere del Parlamento, nel ratificare le sue direttive, ma non è tenuta a farlo alla lettera. In più, ogni Parlamento nazionale dovrà approvare leggi che rispettino le direttive della Commissione.

Anche il parziale successo ottenuto quindi al Parlamento Europeo (parziale perché, comunque, non tutti i punti contestati sono stati esclusi dal testo finale), rischia di essere una vittoria di Pirro.

Però da tutto questo abbiamo imparato qualcosa: se stiamo attenti a ciò che succede nel mondo della politica, possiamo accorgerci in tempo quando i potenti cercano di cancellare un diritto, o di sottrarci delle libertà. E una volta scoperti, possiamo fare abbastanza rumore da farci sentire, e condizionare le loro scelte.

La prima parziale vittoria deve quindi servire come stimolo a tenere alta la guardia, e sorvegliare tutti i prossimi appuntamenti nel corso dell'iter di queste leggi, a ogni livello. Noi non molleremo: saremo sempre qui, a tenervi informati su ciò che succede. Senza vincoli né peli sulla lingua.

grand@hackerjournal.it

FREE HACK NET

Saremo di nuovo in edicola Giovedì 23 ottobre !

Tornano gli abbonamenti!

Abbonati a Hacker Journal !

25 numeri della rivista + il mitico "CAPPELLINO" HJ con ricamato il logo di HJ al prezzo di € 50,00

Dopo un periodo di pausa, tornano alla grande i servizi di abbonamento e arretrati. La gestione non sarà effettuata dalla redazione, ma da una struttura esterna, che accetterà pagamenti in conto corrente postale o via carta di credito. Per informazioni, bisogna contattare la Staff srl ai seguenti recapiti:

Tel. 02/45702415 (dal Lunedì al Venerdì,
ore 9.30/12.30 - 14.30/17.30)
Fax 02/45702434
abbonamenti@staffonline.biz

Potete trovare i moduli da compilare e tutte le istruzioni all'indirizzo:
www.hackerjournal.it/abbonamenti



FREE HACK NET



freeHACKnet è il servizio gratuito di collegamento a Internet targato Hacker Journal: indirizzo email @hackerjournal.it con 5 Mbyte, accesso super veloce fino a 128 Kbit al secondo (ISDN multilink PPP), server newsgroup, controllo anti virus e anti spam. Niente abbonamento, nessuno sbattimento, paghi solo la tariffa telefonica urbana. Corri subito a iscriverti su **www.hackerjournal.it/freeinternet**

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: pizzic8
pass: vi3o

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

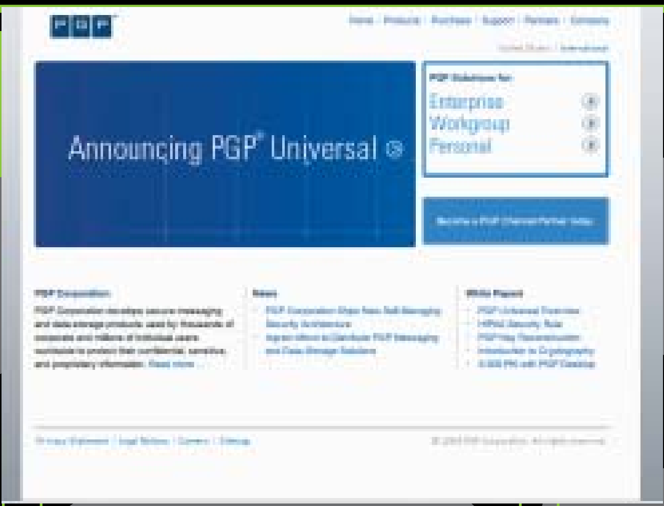
mailto:
redazione@hackerjournal.it

EMAIL SICURE IN ITALIANO

Nel n.31 avete fatto notare ad un'altro lettore la possibilità di avere un' e-mail sicura con il servizio di hushmail.com... la mia domanda è questa: esiste un altro servizio che offre la stessa cosa ma in italiano? oppure esiste qualche programma abbastanza potente che fa la stessa cosa sempre in italiano?
un saluto a tutti e... COMPLIMENTI PER TUTTO...

xtotemx

In effetti, trovare qualcosa di simile in italiano è abbsatanza raro. Solitamente, l'utilizzo di una connessione cifrata per le email è confinata nell'ambiente universitaro, o aziendale. Neanche i provider a pagamento supportano l'uso di SSL nel download della posta (neppure Fastweb, nonostante l'elevato costo dell'abbonamento). Solo qualche società di hosting tra le più serie annovera questo servizio nei suoi listini. Puoi porvare a spulciare su http://hosting.html.it le schede dei vari provider, fare un po' di ricerche, oppure chiedere sul nostro forum.
In alternativa, puoi pensare di usare programmi come PGP/GPG, che però richiedono che anche il destinatario usi lo stesso tipo di programma, e comunque non sono in grado di proteggere informazioni come: nome del destinatario, soggetto del messaggio, data di invio e - cosa molto importante se devi usarlo in una rete aziendale/scolastica - le password di accesso.



RADIO BACCANO

da quasi un anno è venuta ad abitare nell'immobile vicino al mio una tizia che non sa nemmeno dove stia di casa il rispetto per gli altri, ogni mattina circa alle 5 accende la radio ad un volume che mi fa sobbalzare dal letto e a nulla sono valse le mie proteste, se non a prendermi degli insulti, ora per non farvela troppo lunga nel raccontarvi tutte le ozioni legali che ho tentato invano, ho la possibilità di zittire la sua radio coprendole le frequenze?.

Giorgio S.

In teoria dovresti procurarti un trasmettitore FM tarato sulla stessa frequenza della radio preferita sulla tua vicina, e usarlo per trasmettere... silenzio.
In pratica, non è molto semplice coprire un potente trasmettitore di una radio commerciale. La cosa che però deve farti desistere è che così facendo, stai occupando illegalmente una frequenza concessa in uso della radio in questione. Violeresti la legge, insomma.



DISTRIBUIRE PROPRI MP3

Sono webmaster di un sito di un gruppo musicale che ancora non possiede contratto e non è iscritto alla siae (siaaaargggghh, dovremmo dire, dato che costa un ABISSO iscriversi!!).
DOMANDONE: se io metto LORO mp3 nel sito faccio reato e mi fanno il c**o?
Come e dove posso trovare informazioni a riguardo? potete aiutarmi? Per adesso ho tolto gli mp3 "per sicurezza", ma mi spiace un casino...

Tore MaYh3m

Non c'è nessun problema a distribuire Mp3 di brani propri, o di persone o gruppi di cui si abbia l'autorizzazione (in questo caso, il sito è il loro, addirittura). Il problema è se i diritti sono stati ceduti a una casa discogra-

PRECISAZIONE SU CRYPTO MATRIX"

Nel numero 33 di hj a pag. 29 nell'articolo "crypto matrix" c'è un piccolo errore nel definire la conformabilità di due matrici alla moltiplicazione. Nell'articolo è scritto che due matrici sono conformi se il numero di righe della prima è uguale al numero di colonne della seconda.
In realtà due matrici sono conformi nel caso opposto; il numero di colonne della prima deve essere uguale al numero di righe della seconda. Sicuramente sarà stato un errore di distrazione ma è bene precisare.

ed_r4d1cal



fica (ma non mi pare il caso), o se i brani sono stati registrati alla SIAE.
Quando si registra un brano alla SIAE, si incarica questa società di tutelare i propri diritti, e quindi l'autorizzazione alla distribuzione online deve passare attraverso l'Ufficio Multimedialità della SIAE. Nelle Faq del sito siae.it, alle sezione Ufficio Multimedialità, si legge infatti:
Domanda: Sono stato autorizzato direttamente dagli autori ad utilizzare on line le loro opere: devo comunque rivolgermi alla SIAE per la Licenza?
In questo caso si dovrebbe distinguere:
**** se l'autore non è associato o mandante della SIAE o delle Società d'autori estere, l'autorizzazione può essere concessa direttamente da lui stesso;***
**** se l'autore è rappresentato dalla SIAE l'autorizzazione va richiesta alla SIAE stessa, cui è stata affidata in esclusiva la tutela delle opere.***

BLACK OUT DEI CERVELLI

L'altra sera stavo guardando Saturday Night Live su La7 quando all'improvviso si è spento tutto. Guardando il buio totale fuori dalla finestra, e sentendo il coro di allarmi che arrivava da ogni angolo di Milano, mi è stato subito chiaro che non si trattava di un black out normale. La mattina dopo, la conferma è arrivata dai telegiornali, e dai siti Internet che funzionavano (caspita... Repubblica non è stato aggiornato per un bel po', nonostante i server funzionassero regolarmente).
Non voglio mettermi a fare commenti sullo scaricabarile delle istituzioni, o sulle motivazioni davvero poco chiare di una catastrofe energetica di queste proporzioni (a me, le spiegazioni ufficiali non mi hanno convinto per niente...).
Però è indubbio che quando capitano cose come queste ci si rende conto di quanto tutti quanti dipendiamo dalla tecnologia, e questa dall'energia. Niente corrente, vuol dire niente informazione (né possibilità di produrla), niente comunicazioni, spostamenti difficili. Ora, il coro dei potenti intonava l'aria -già sentita in occasione delle interruzioni estive- che più o meno fa "ci servono più Centrali. Magari nucleari". A nessuno viene in mente che, magari, si può anche fare qualcosa per risparmiare? Per esempio, non lasciare gli elettrodomestici (tv, computer e videoregistratori) in stand-by, ma spegnerli con interruttore. Alcune periferiche, per esempio, non hanno nemmeno un interruttore di accensione che stacca effettivamente l'alimentatore dalla rete, e quindi continuano a consumare anche quando sono spente.
Oggi, poi, il collegamento tra paio di notizie mi ha lasciato sgomento. Un responsabile dei sistemi informatici della Borsa di Milano, nel dichiarare che il black out non ha causato nessun disservizio ai sofisticati sistemi informatici che regolano gli scambi commerciali, ha precisato che i generatori di energia in dotazione alla borsa hanno carburante a sufficienza per far funzionare il tutto a pieno regime per una settimana. So che anche i migliori provider possono vantare simili caratteristiche (i.Net, sul suo sito, dichiara dieci giorni di autonomia). Ora, sapendo che questi standard di affidabilità si possono ottenere, e sono dati per scontati in servizi di questo tipo, mi domando: "come mai i pompieri di alcune citta, come per esempio Roma, hanno dovuto consegnare gasolio agli ospedali, perché i loro generatori avevano autonomia di poche ore? Davvero la vita umana vale così poco in confronto alle transazioni finanziarie?".

Gino. O'Knaus

Che dire, caro Gino, non possiamo che concordare con te nel biasimare la miopia degli amministratori di quegli ospedali.

Tech Humor

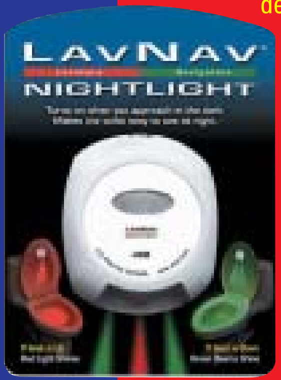
Vi racconto la storia di un lamer, che io e i miei amici chiamiamo, da quell'episodio, "Il Programmatore".
Di seguito il discorso:
-DeeJayAndrea(io): Sai programmare in Java?
-"Il Programmatore": Certo! È una stupidaggine.
-DJA: ah, anche te? senti, io non mi ricordo una cosa: qual'è il codice per stampare le parole a schermo?
-"IIP": mmm... mi sembra rt53t7... ora non mi ricordo...
-DJA :...
Ora comincio a bluffare, e lui ci casca in pieno:
-DJA: Com'era quello per ottenere da stack dell'overrunning il sovrabasso del glosting?
-"IIP": Si, lo so, aspetta, ora non mi ricordo..

NEWS

HOT!

MAI PIÙ FUORI DAL BUCO

Chi non ha rischiato almeno una volta di sbagliar mira mentre si apprestava a fare ehm, certi scroscianti bisogni nel cuore della notte? Una ditta californiana che ha preso molto seriamente tale inconveniente, ha pensato a una brillante soluzione. Inventare un marchingegno che, tramite un sensore installato alla base del WC, rileva il nostro avvicinamento e accende una luce sulla tazza. Rossa se la tavoletta è sollevata, un avvertimento per il genti sesso. Verde se è abbassata, un avvertimento per i signori maschietti che faranno bene ad alzarla prima di liberarsi, onde evitare successive estenuanti discussioni sull'argomento con le donne di casa. Questa furbata permetterà inoltre di raggiungere l'anelato luogo senza accendere altre luci, dunque senza rischiare che familiari disturbati nel sonno e imbufaliti ci tirino ciabatte e quant'altro. L'oggetto si chiama LavNav e costa solo 30 dollari.



ADDIO COCCINELLE

Altro che le coccinelle e ammennicoli vari a calamita che fino a qualche tempo fa andavano di moda per difenderci dai campi elettromagnetici generati dai cellulari. Roba superata. Negli Stati Uniti stanno mettendo a punto un orologio che funziona da schermo totale contro l'inquinamento elettromagnetico di telefonini, computer e simili. Un chip interno genera frequenze che vanno a neutralizzare quelle dannose per la nostra salute. Funzionare funziona. Parola di chi lo ha provato: meno stanchezza, niente mal di testa, migliori prestazioni. E se anche non funzionasse, poco male: ha un look così trendy, che non rimpiangeremmo la somma sborsata.



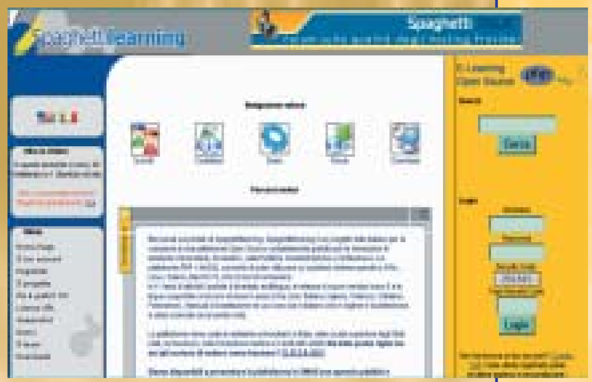
IL GRANDE GENITORE



Altro che Grande Fratello! Il lungo braccio del controllo di mamma e papà si avvia a divenire un mostro tentacolare. Tutto per colpa della tecnologia.
I cellulari ci rendono sempre raggiungibili, le pagelle elettroniche e il registro delle assenze online non ci permettono più di farla franca. E ora dagli Stati Uniti sta arrivando la RS-1000 Black Box, una specie di scatola nera da mettere sull'auto che registra tutte le malefatte automobilistiche, per fortuna solo quelle, dei figli sciagurati. Verranno memorizzate infrazioni dei limiti di velocità, mancato allacciamento delle cinture, curve troppo brusche. Ci sarà persino un resoconto della strada percorsa. Che significa che ogni volta che invece che in biblioteca a studiare, andremo a svaccarci al parco o a infrattarci con la fidanza, mammà lo verrà a sapere. Una pestilenza. Ma non è finita. Per riportare alla disciplina guidatori troppo sportivi la Black Box dispone di un segnalatore acustico che avverte dell'infrazione. Inutile cercare di mettere a chiodo l'autoradio: il volume del gendarme elettronico si alzerà di conseguenza. È la fine. Ma giacchè si dice che "a mali estremi, estremi rimedi", quanti giorni dovranno passare prima che la scatola nera venga hackerata? Si accettano scommesse.

SPAGHETTI PER L'ISTRUZIONE

Piatto goloso sul tavolo dell'insegnamento a distanza. Realizzata da Spaghetti Learning, gruppo di lavoro completamente italiano, è da poco disponibile una piattaforma per e-learning Open Source gratuita. La piattaforma è l'ideale per gestire progetti di formazione a distanza in tutti gli ambiti: lavorativo, scolastico, universitario e della pubblica amministrazione. Le principali funzionalità della piattaforma sono: impostazioni e monitoraggio dell'attività utente; supporto lezioni anche multimediali; test; interazione docente-allievo basato su chat e forum. Chi fosse interessato troverà tutte le informazioni necessarie sul sito all'indirizzo www.spaghettilearning.com Per avere un'idea concreta del prodotto e delle sue applicazioni dalla home del sito è possibile scaricare una demo.



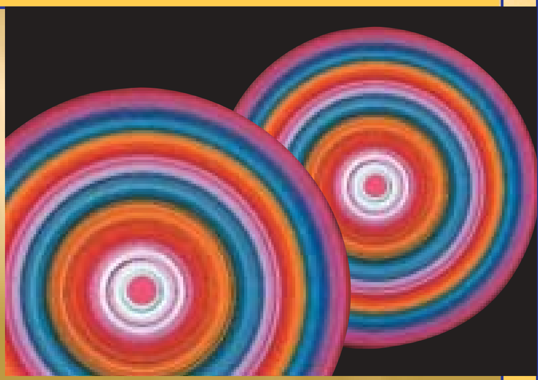
PROIBITO CONDIVIDERE

Anche se non siamo fan dell'artista soul Anthony Hamilton, l'uscita del suo ultimo disco lo scorso 23 settembre, dovrebbe averci fatto alzare le antenne. Motivo? Le nuove protezioni prodotte da SunnComm e inserite nell'album dalla casa discografica Arista Records, divisione di BMG. Il sistema di protezione adottato è piuttosto diverso dai precedenti. E soprattutto ha l'aria di voler dare un contentino al pubblico, cercando di ingraziarselo con qualche concessione in più. Il cd contiene infatti file in mp3 da scaricare sul computer, che però sono codificati in maniera tale da impedire alcune operazioni tra cui la condivisione.
In compenso, chi acquista il CD potrà masterizzare tre copie delle canzoni. Il disco fornirà inoltre un collegamento di condivisione che permette lo scaricamento dell'album da parte di altre persone e il suo ascolto per soli dieci giorni.



NUOVI CD STESSA FREGATURA

Le case discografiche non si rassegnano. Soprattutto fanno finta di non capire che le vendite dei CD forse sono crollate perché ormai per comprane uno bisogna chiedere un fido alla banca. Allora per aggirare il problema cosa fanno? Ne pensano di tutti i colori. L'ultima trovata di Warner e Sony è il dual disc, un nuovo supporto che da un lato, su cd, contiene le tracce audio dall'altro, su dvd, i video degli artisti. Naturalmente il dual disc costerà come prima o più di prima. Dunque cosa si risolverà? Niente. Meditate signori discografici, meditate.



FINALMENTE UN WORM BUONO



Niente a che vedere con i virus informatici. Il worm di cui parliamo lo hanno inventato a Tokyo, si chiama Koga ed è un vermiciattolone telecomandato che, portato sul teatro dei terremoti, aiuterà i soccorritori a individuare persone ancora in vita sotto le macerie. Koga ha una telecamera montata sulla testa e si sposta in maniera appositamente studiata per non generare crolli. L'unica pecca del bruco da soccorso è la resistenza. Le batterie durano infatti solo 30 minuti.
Koga non è unico nel suo genere, ha anche una "cugina": Moira, un prototipo analogo lungo quasi un metro e mezzo, realizzato dall'Università di Kyoto.

DIALER? NO GRAZIE!

Annebbiati dai fumi del coinvolgimento dei giochi online, anche ai più sgamati almeno una volta può succedere di cadere nella trappola dei dialer. Col risultato di vedersi recapitare bollette telefoniche che stenderebbero anche un bisonte. Per giocare online senza lo stress di ricevere fregature, adesso c'è un portale sicuro. Si chiama Giochi.org e lo troviamo all'indirizzo internet www.giochi.org. I giochi sono tutti in flash, commentati in italiano e divisi per categorie. Presto verrà inaugurata una sezione di giochi multiplayer e una di giochi da usare con telefonini e palmari.

LAUREA IN SICUREZZA INFORMATICA

Da quest'anno chi ha sempre avuto il pallino della sicurezza informatica potrà trasformare la sua passione in un bel certificato di laurea. Bastano tre anni di corso presso il polo universitario Cremasco dell'Università di Milano, ed eccoci togati Dottori in Sicurezza dei sistemi e delle Reti informatiche. Le materie di studio sono molto varie, alcune strettamente tecnico-pratiche, altre di più ampio respiro. Algoritmi e strutture dati, crittografia, diritto dell'informatica, finanzia aziendale solo per citarne alcune tra le tante. Di sicuro il corso di laurea garantirà buoni sbocchi professionali. Con i tempi che corrono un buon esperto di informatica, di reti di computer e di lotta alle i intrusioni nei sistemi informatici, non tarderà a trovare lavoro. Per avere maggiori informazioni e per consultare il piano di studi colleghiamoci al sito della facoltà: http://www.dti.unimi.it/corso.php?z=0;id_corso=7

HOT!

A SCUOLA DI LINUX



Autunno è tempo di corsi di ogni genere. Perché non cimentarsi in un corso di Linux. Ne abbiamo scovati alcuni completamente gratuiti, uno dei quali finanziato da Unione Europea, Fondo sociale Europeo, Ministero del Lavoro e Regione Lombardia. Il corso è destinato a 12 diplomati, in cerca di prima occupazione, iscritti alle liste di mobilità o studenti. Tra gli argomenti affrontati nelle lezioni: visione di insieme del sistema operativo, configurazione della rete, installazione e aggiornamento del software, utilizzo dei principali servizi, analisi del boot dei processi e della rete e molto altro ancora. Al termine del corso ai partecipanti verrà rilasciato il certificato di qualifica di secondo livello.
Per ulteriori informazioni: sistema imprese sociali-settore formazione: e-mail segformazione@consorziosis.org
Tel. 02.2688.011



LINUX, L'ALTERNATIVA INFORMATICA

L'iscrizione è aperta indifferentemente ai soggetti occupati e in cerca di occupazione. Il corso è finanziato dal Fondo Sociale Europeo ed è completamente gratuito.
Luogo del corso: Pordenone
http://www.ialweb.it/shownews.asp?idnews=634

TECNICO DI SISTEMA E NETWORKING LINUX

Luogo del corso: Milano
http://www.formazionein.it/site/dettaglio_corso.asp?id_formazione=366

SISTEMISTA IN AMBIENTE LINUX

Luogo del corso: Legnano
http://www.campusnet.it/corsi2003_2004.asp



HACKER C

Esistono molte tipologie di hacker, ma c'è un sistema di valori, un codice non scritto che tutti gli hacker condividono. Questi valori rappresentano il vero collante della cultura hacker

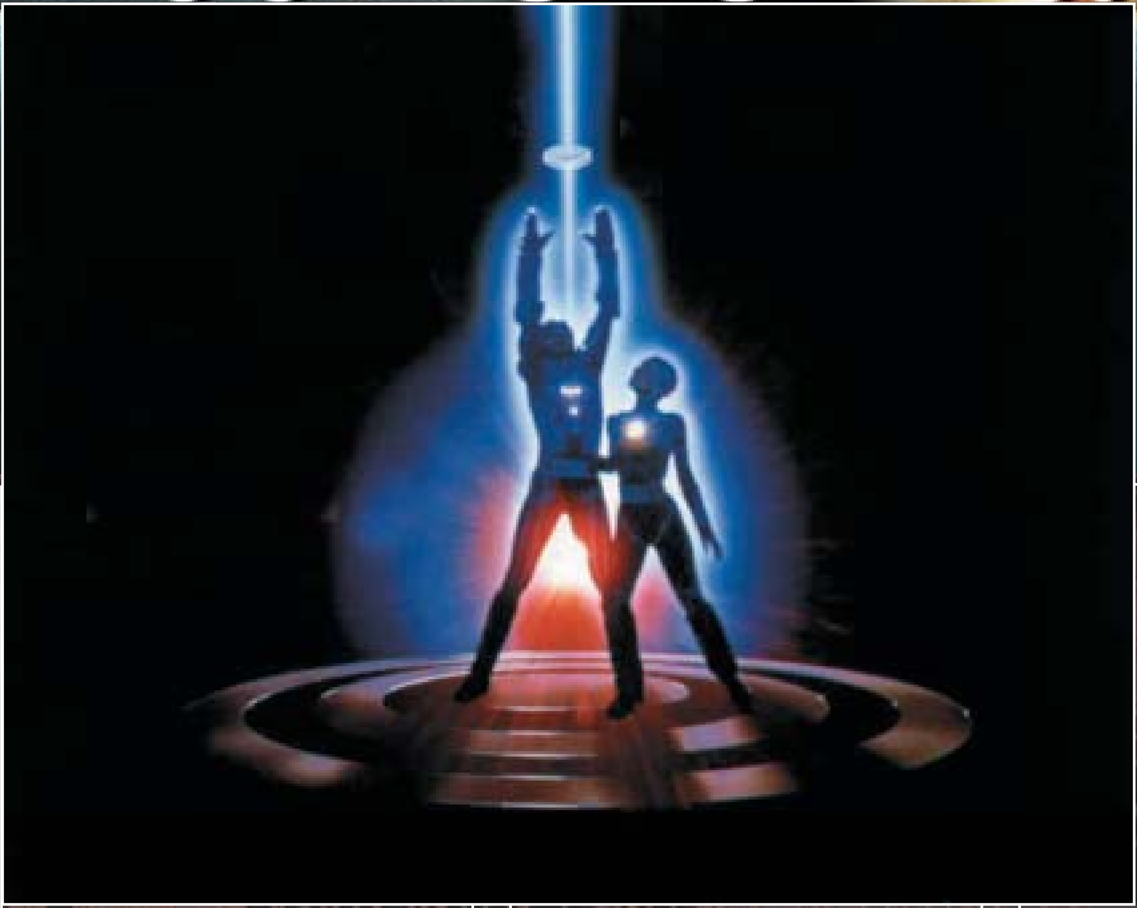
Tracciare un'immagine assoluta dell'hacker o elencare in poche righe le sue molteplici attività non è possibile. **Non tutti gli hacker sono uguali**, non tutti gli hacker la pensano allo stesso modo, hanno gli stessi interessi o fanno le stesse cose. Eppure **i media ufficiali descrivono l'hacker come un geek**, un individuo ossessionato dai computer, che trascorre la maggior parte del suo tempo nella Rete, un vero esperto di reti e programmazione, un professionista hi-tech **o, peggio ancora, come un criminale o cracker**. Mai una volta che si mettessero da parte le etichette e i cliché e si parlasse dei valori degli hacker e di hacking in termini di cultura e non solo di competenza tecnica. Tutto questo non è casuale!

>> Le culture

Chi pretende di dare una definizione univoca di hacker o di hacking, **dimentica molto spesso di considerare le diverse culture cui gli hacker appartengono** e che hanno fatto sì che l'hacking si sviluppasse, dagli anni '50 a oggi, in maniera assai variegata. Il modo di concepire l'hacking, gli stessi atteggiamenti degli hacker cambiano infatti da paese a paese. Ed è sempre stato così! Ad Amburgo gli Hacker del "**Chaos Computer Club**" erano più interessati a distribuire informazione e conoscenza tra le masse, ed hanno infatti lanciato il social hacking. Gli americani, quelli della conferenza "**Hope - Hackers On Planet Earth**", erano attratti dalla sfida tecnologica ed hanno scritto software libero e non commerciale. Gli hacker europei, dei meeting olandesi dell' "**Icata '98**", di "**Hacking in Progress**" e degli "**Hackmeeting**" Italiani, si sono distinti e si distinguono tuttora per l'attivismo e l'accanita lotta al copyright e ai brevetti.
La scena italiana, mostra dei tratti peculiari, assolutamente distinti da quelli del resto d'Europa. In Italia, come è spiegato in **Hacktivism** di **A. Di Corinto e T.Tozzi**, un libro che ripercorre anche la storia del movimento hacker italiano, "l'uso dei computers si è incontrato con la filosofia comunitaria



culture e valori

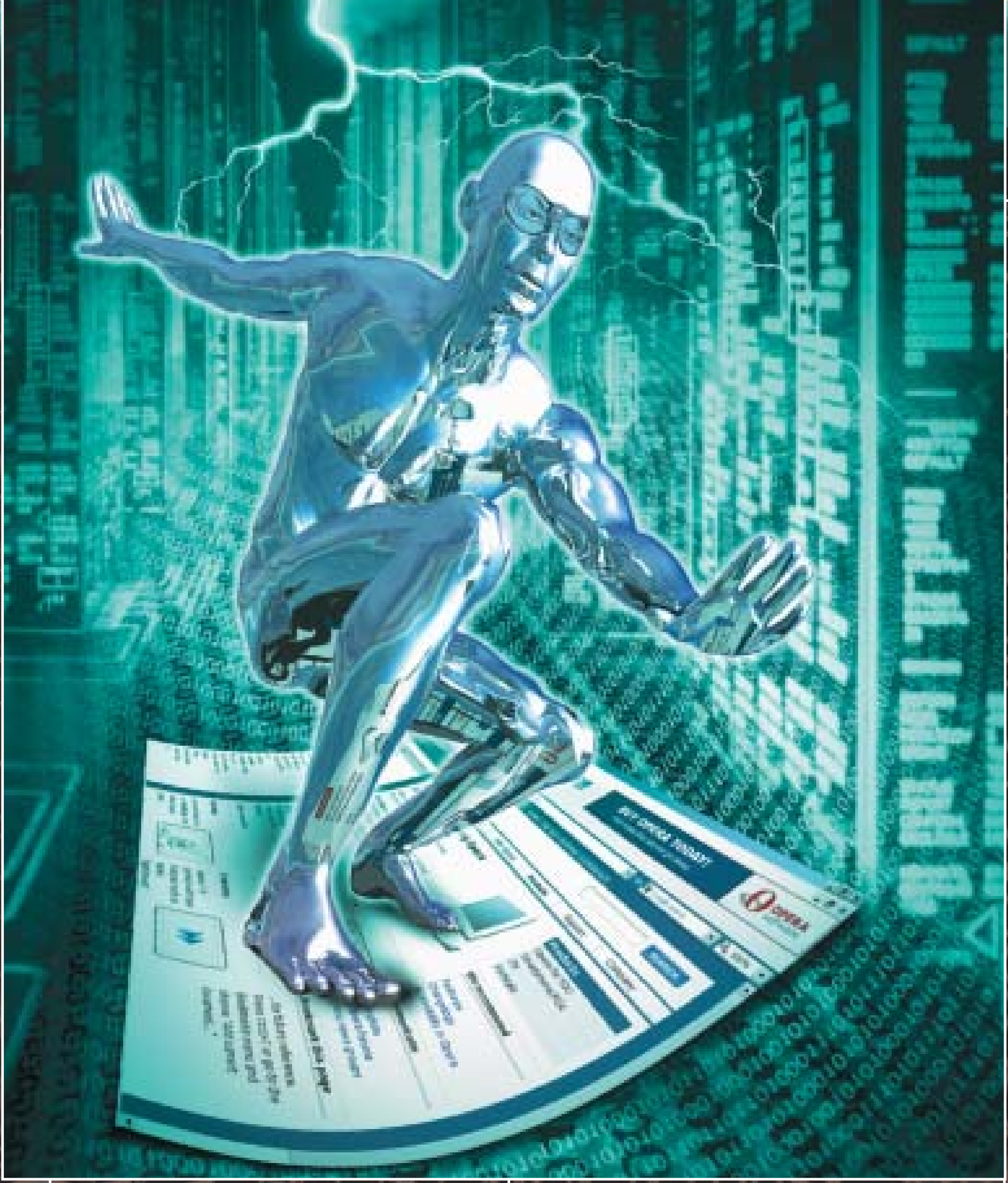


dei primi Bulletin Board System, e la pratica autogestionaria dei centri sociali ha dato vita ai numerosi hacklabs tutti impegnati nella democratizzazione delle tecnologie informatiche". Stéphane Mandare, in un articolo su Le Mond, scrive che gli hacker italiani si caratterizzano per una maggiore coscienza sociale e per un'accanita militanza in rete. Danno molta più importanza all'-hacking come attitudine piuttosto che agli aspetti tecnici, anche se tra loro vi siano dei veri esperti. Concepiscono l'-hacking come un'etica basata sulla condivisione delle conoscenze. Non sono quindi nerd, né pericolosi pirati che penetrano nei sistemi per distruggere o rubare informazioni riservate.

>> Le tipologie

Tutti gli hacker sembrano d'accordo riguardo ad un "**uso non convenzionale dei computer**", ma non sempre sono degli esperti informatici. Tutti sono convinti, inoltre, che lo scopo ultimo dell'hacking sia "**migliorare qualcosa**", ma non tutti desiderano migliorare la stessa cosa, nello stesso modo e con gli stessi mezzi. "Migliorare", inoltre, non ha lo stesso significato per tutti. Per alcuni vuol dire **aggiustare**, per altri **modificare**, **deformare** o **distruggere**. C'è, ad esempio chi è più interessato a "mettere le mani sopra" a un sistema per il puro gusto di modificarlo, scoprirne le imperfezioni e correggerlo. C'è l'hacker sociale per il quale ogni controllo sull'informazione è negativo e quindi **impiega l'hacking per abbattere ogni barriera che separa le persone dalla conoscenza**. Ci sono quelli, definiti in Haktivism "moderni Robin Hood della comunicazione", che svaligiano la banca dell'informazione per restituire alla comunità ciò che gli è stato sottratto dalle leggi di protezioni del software o delle opere dell'ingegno. C'è anche chi intende l'-hacking come "**reinterpretazione funzionale**" di parole e di concetti o un'operazione di "deturpamento", cioè di modificazione del senso. Il **Defacement**, ad esempio, è una forma di deturpamento: consiste, infatti, nella sostituzione del contenuto di un sito con un altro contenuto.

Per alcuni hacker il diritto alla "deformazione" è importante quanto il diritto all'"informazione". Con la deformazione si possono rendere note o criticare le contraddizioni e le azioni dei proprieta-



ri dei siti, in genere multinazionali, istituzioni economiche o politiche; si può stimolare una riflessione critica sul concetto di informazione. La deformazione è anche concepita come una nuova forma di cooperazione tra la gente. "E' come costruire, sostiene W. Holland, una bottiglia partendo dal materiale grezzo e fuso: con le tue mani attraverso il processo di informazione tu dai una forma precisa a quel materiale che prima era non in forma e deformandolo otterrai la tua bottiglia, otterrai cioè uno strumento per scambiare idee".

>> La comunità

Esistono diverse culture hacker e anche diversi modi di intendere l'hacking. Tutti gli hacker però sono indissolubilmente legati tra loro da un comune denominatore, **da qualcosa che, al di là delle differenze, li fa sentire parte di un'unica grande comunità e di un'unica grande cultura**. Questo comune denominatore, purtroppo, è stato ed è tuttora erroneamente identificato, persino dai giovanissimi che popolano più di altri chat

Bibliografia e "sitografia" ;-)

Hacker attitude - Stéphane Mandard
http://www.mafhoum.com/press4/117T44.htm
Traduzione italiana
http://lists.kyuzz.org/pipermail/hackmeeting/2002-December/000116.html
Hacktivism. La libertà nelle maglie della rete - A. Di Corinto e T. Tozzi
http://www.hackerart.org/storia/hacktivism.htm
Gli hackers come controcultura tra identità e rappresentazione – Federica Guerrini
http://space.tin.it/spettacolo/fguerrin/frmain02.htm
Chaos Computer Club
http://www.ccc.de
Hackers On Planet Earth
http://www.h2k2.net
Galactic Hacker Party (Icata 89)
http://wiki.camp.ccc.de/Camp/view/Main/GalacticHackerParty1989
Hacking in Progress
http://www.hip97.nl
Hackmeeting Italiani
http://www.hackmeeting.org
Software libero
http://www.gnu.org
http://www.fsfeurope.org
http://www.fsfeurope.org

room, mailing list e gruppi di discussione, con la "sconsiderata passione" per i computer, la rete e la tecnologia in generale e la "competenza tecnica" in campo informatico. Questo fa sì che agli hacker venga attribuita spesso l'etichetta di geek, cioè di **persona disadattata, socialmente inquieta ed anticonformista**, ma eccezionalmente appassionata di computer e amante della telematica, che chiunque sia uno smanettone o abbia semplicemente una particolare predisposizione per i computer o la programmazione, oppure sia riuscito almeno una volta a defacciare un sito o ad entrare nel computer di qualcun altro si senta un hacker o venga considerato tale da chi, in genere, ne sa di meno: l'amico incompetente e i media ufficiali. "Di fatto hacker, si spiega in Hacktivism, è un termine la cui definizione non può essere applicata a un caso singolo, in quanto hacker si è all'interno di una collettività. Una moltitudine talmente variegata che al suo interno è in grado di contenere figure specializzate non solo nel campo tecnico, ma anche in quello politico, artistico, filosofico, psicologico, sociologico, mediologico, giuridico, umanitario, ecc., ed ognuna di queste persone diventa, nel gruppo, un hacker". L'hacker è "**un esperto o entusiasta di qualsiasi tipo**" (significato 6 del Jargon File) ed è forse anche per questo che la scena hacker ha abbracciato persino sfere apparentemente distanti da quella tecnologica, sviluppandosi in maniera assai complessa oltre che variegata.



>> I valori

Il vero collante della cultura hacker, quel comune denominatore di cui parlavamo che fa sentire tutti gli hacker parte di un'unica grande comunità, è l'etica hacker. Essere un "vero hacker", scrive **Federica Guerrini** in Gli hackers come controcultura tra identità e rappresentazione, implica soprattutto condividere un sistema di valori, una mentalità e un modello di vita. Questo "sistema di valori profondi" è sia "un codice di responsabilità", che una "filosofia di socializzazione, di apertura, di decentralizzazione".

Oggi persino i ragazzini sanno entrare nei sistemi informatici altrui e sono sempre di più quelli che, conoscendo delle tecniche hacker ed essendo come gli hacker altrettanto preparati sul piano della sicurezza informatica, utilizzano le proprie conoscenze per fini illeciti. Ciò che distingue un hacker, da un comune criminale o un semplice smanettone **non è quindi il mezzo e la competenza tecnica, ma il sistema di valori e il fine.** Ed infatti, per i primi hacker come per quelli di oggi, i computer e le reti telematiche sono solo degli "**strumenti**" per realizzare ciò che considerano un diritto umano fondamentale: l'accesso illimitato all'informazione.

Se i media ufficiali preferiscono le etichette e le definizioni, piuttosto che considerare questi valori, c'è una ragione. I principi dell'etica hacker - **l'accesso ai computer deve essere illimitato e completo**, **tutta l'informazione vuole e deve essere libera**, **dubitare dell'autorità e promuovere il decentramento**, **con i computer si può cambiare la vita in meglio** – vanno contro l'interesse delle multinazionali e delle grandi aziende del software, contro il monopolio, il colonialismo culturale e quindi non se ne deve parlare, non vanno diffusi. La comunità hacker "si oppone alla cultura dominante anche in forme dichiaratamente politiche e ideologiche (coscienza politica, coerenza filosofica, manifesti, in sintesi un'etica) e mette in opera istituzioni "alternative" (stampa underground, gergo, propri spazi simbolici e fisici)". Rappresenta, insomma, una vera e propria "controcultura", "un movimento, spiega ancora Guerrini, con vocazione antagonista e neo-underground che si prefigge l'obiettivo di annullare l'abuso del potere sui cittadini e di sostituire rivoluzionari modelli di pensiero e comportamento a quelli dominanti".

DaMe`
dame@dvara.net



BANCOM

Il vostro bancomat può essere clonato, e il suo PIN craccato in 15 tentativi. Le banche lo sanno, ma la loro unica preoccupazione è che non veniate a saperlo VOI!

"Nell'ultimo estratto conto della mia banca ho trovato gli addebiti di alcune voci di spesa effettuate tramite POS in negozi in cui non sono mai stato (addirittura alcuni in luoghi che non conosco!)".

"Mi hanno rubato il portafogli con tre tessere bancomat; in meno di un'ora i ladri avevano già esaurito tutte le passibilità di credito (prelievo, acquisti POS, presticash), ma ovviamente i PIN non erano conservati nel portafogli".

"Nei mesi scorsi mi sono visto addebitare migliaia di euro in prelievi bancomat effettuati dalla Spagna, ma io non ci sono mai stato!"

Sui newsgroup it.discussioni.consumatori.tutela e it.comp.sicurezza.varie capita di leggere messaggi come quelli che abbiamo citato qui sopra. Altre segnalazioni di utenti bancomat o carta di credico con problemi simili le abbiamo raccolte direttamente. Sui newsgroup, **i primi messaggi risalgono al 2001**, quindi è da tempo che in **Italia esistono casi di prelievi fantasma**, o comunque di utilizzo illecito del bancomat. Di fronte a situazioni di questo tipo, la banca in genere attribuisce l'illecito ad incuria dell'utente dal momento che, anche qualora un criminale riuscisse a copiare il contenuto del nastro magnetico di un bancomat attraverso un POS modificato, **non avendo il PIN, non potrebbe prelevare o utilizzare in alcun modo la carta**. Per cui in questo caso è l'utente a rendere noto anche involontariamente il suo PIN al criminale…

>> ...fino a prova contraria!

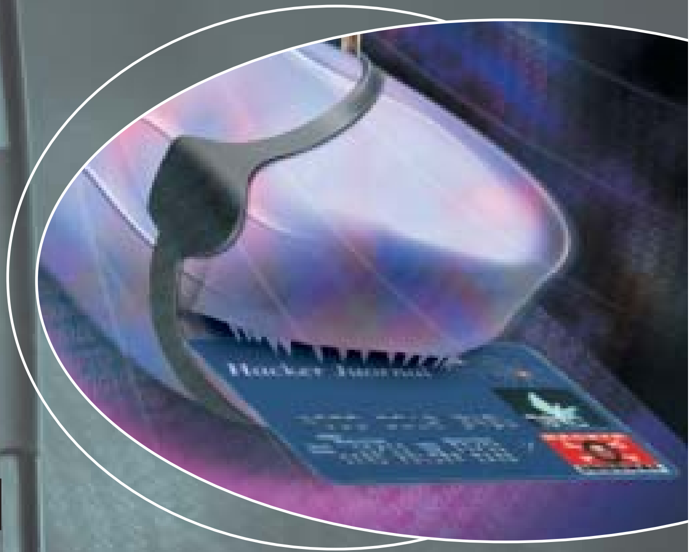
Una disavventura del genere è capitata circa un anno fa anche ai coniugi **Singh**, cittadini britannici, residenti a Londra, che si erano concessi un weekend in Sud Africa. **In loro assenza erano stati effettuati dei prelievi a Londra con il loro bancomat e il loro PIN**. Da questo episodio è partita una causa legale tra la **Diners/Citibank** e i Singh, i quali, per dimostrare che ricavare il PIN di una carta ATM (i bancomat internazionali) non è impossibile, si sono rivolti al **Prof. Anderson** del dipartimento di sicurezza informatica e crittografia del **computer laboratory dell'Università di Cambridge**. Quest'ultimo ha affidato il lavoro ad un suo studente Mike Bond il quale, dopo un'analisi approfondita ha stilato un rapporto tecnico reperibile al seguente indirizzo: http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf .

In questo rapporto viene innanzitutto descritto il funzionamento del sistema IBM 3624 implementato dalla Citibank, sono messe in evidenza le vulnerabilità e sono descritti tre algoritmi di cui il migliore **è in grado di trovare un PIN dopo appena 15 tentativi** a fronte dei 5000 che statisticamente potrebbero portare al medesimo risultato con un attacco a forza bruta. Il PIN delle carte ATM e delle carte di credito, infatti, è costituito da **4 cifre**. I caratteri previsti sono soltanto numerici ossia 10: **1234567890**. Le combinazioni possibili sono quindi **10 ^ 4 cioè 10.000**. Per trovare quindi un PIN valido relativamente ad un particolare conto corrente sono necessarie almeno metà delle combinazioni ossia 5000 per avere il 50% di probabilità di trovarlo.

UNIVERSITY OF CAMBRIDGE



AT, PIN E



PRELIEVI FANTASMA

>> Verifica del PIN con sistema IBM3624

Quando l'utente inserisce la sua carta nell'apposita fessura del bancomat il sistema legge dalla striscia magnetica il numero di conto corrente dell'utente. A differenza di quanto si possa pensare **il PIN non è presente nella striscia magnetica né cifrato né tanto meno in chiaro**. Una volta che l'utente inserisce il PIN con la tastiera numerica, i dati vengono inviati all'**HSM** (**Hardware Security Module**) che è un coprocessore su cui gira una API relativa ai servizi finanziari ed, in genere, è unico per ogni banca. L'HSM possiede varie funzioni di libreria che ad una richiesta esterna rispondono esclusivamente con un no o con un sì. In particolare quella che si occupa dell'autenticazione è la **Encrypted_PIN_Verify** di cui vi riportiamo il prototipo:

```
Encrypted_PIN_Verify(
A_RETRES , A_ED ,                      // return codes 0,0=yes 4,19=no
trial_pin_kek_in , pinver_key ,       // encryption keys for enc inputs
(UCHAR*)"3624 " "NONE "               // PIN block format
" F"                                  // PIN block pad digit
(UCHAR*)" " ,
trial_pin ,                           // encrypted_PIN_block
I_LONG(2) ,
(UCHAR*)"IBM-PINO" "PADDIGIT" ,       // PIN verification method
I_LONG(4) ,                           // # of PIN digits = 4
"0123456789012345"                    // decimalisation table
"123456789012 "                       // PAN_data (account number)
"0000 "                               // offset data
);
```

I tre parametri in ingresso più importanti inviati alla funzione sono:
1 **l'encrypted_PIN_block** che non è altro che il PIN inserito dall'utente sul tastierino dello sportello bancomat, criptato allo scopo di evitare intercettazioni;
2 **il PAN_data** ossia il numero di conto letto sulla carta bancomat;
3 **la decimalisation table**, ossia la tabella di conversione in decimale o tabella di decimalizzazione;

>> L'origine del PIN

Prima di proseguire è opportuno che si sappia come viene generato il PIN a 4 cifre di un bancomat ATM. **Il Pin ha un legame stretto con il numero di conto o il numero della carta di credito**, infatti, esso è costituito dalle prime quattro cifre esadecimali del numero di conto corrente, o della carta, criptato con l'algoritmo DES e con una chiave caratteristica di ogni banca chiamata appunto "**PIN generation key**". Facciamo un esempio:

4556 2385 7753 2239	un ipotetico numero di carta
3F7C 2201 00CA 8AB3	il numero di carta cifrato con DES

Prendiamo le prime 4 cifre che costituiranno il PIN, ossia 3F7C.
A questo punto, entra in gioco la tabella di conversione decimale che fa in modo che il PIN possa essere digitato sul tastierino numerico di un normale sportello bancomat

0 1 2 3 4 5 6 7 8 9 A B C D E F	le 16 cifre esadecimali
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	la corrispondenza con le cifre decimali

Le nostre 4 cifre diventano quindi 3572 **ed ecco ottenuto un PIN valido**. In genere, a ciò si aggiunge anche un valore di offset, ossia un numero di massimo 4 cifre che di base viene impostato a 0000 e che serve qualora l'utente, per qualche motivo, faccia richiesta di un nuovo PIN. Dal momento che non è possibile cambiare il suo numero di conto **ci si limita ad aggiungere un certo valore al Pin originario;** l'offset viene registrato nella carta stessa. Come potete notare, tale valore viene inviato sempre alla funzione di verifica dell'HSM attraverso il parametro **offset_data**.
Per la verifica di una richiesta di prelievo, l'HSM segue il procedimento inverso, ossia sottrae dal PIN l'offset dopodiché converte il risultato ottenuto con la tabella di conversione decimale fornita insieme alla richiesta e confronta il risultato con le prime 4 cifre criptate del conto corrente.
Nell'esempio che abbiamo fatto il PIN 3572 darebbe un risultato positivo non soltanto nel caso in cui le prime 4 cifre esadecimali del conto criptato fossero **3F7C** ma anche **3F72** o **3572**. Insomma, in tutti i casi in cui il PIN inserito abbia una corrispondenza con la tabella di conversione.
Mike Bond sfruttando questa vulnerabilità ha dimostrato che attraverso la manipolazione della tabella di conversione **è possibile ottenere le 4 cifre costituenti il PIN valido** e quindi provando tutte le combinazioni arrivare al PIN stesso.

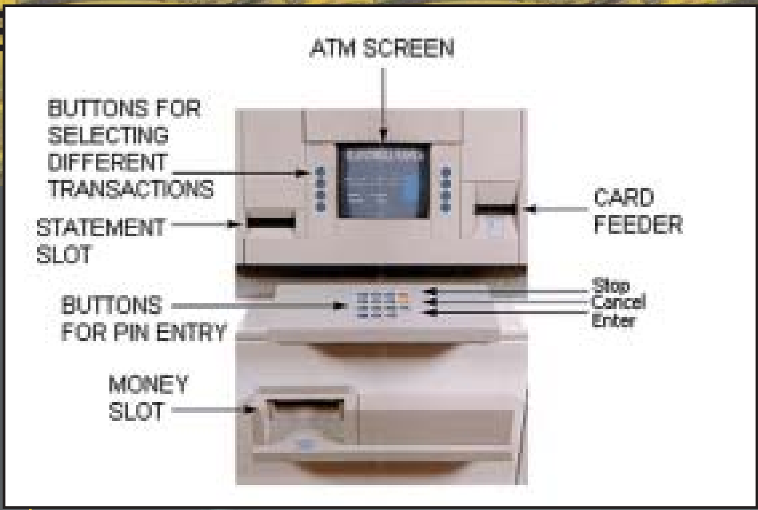
>> Manipolazione delle tabelle di conversione

Ipotizziamo che il PIN originale in esadecimale sia quello dell'esempio e che noi siamo in grado di inviare all'HSM la tabella che desideriamo; nel caso specifico la seguente:

0 1 2 3 4 5 6 7 8 9 A B C D E F
0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0

Inviamo come PIN 0000, insieme al numero di conto corrente di cui volgiamo scoprire il vero PIN. A questo punto l'HSM darà come valido il PIN 0000 soltanto se nel PIN vero sarà presente il numero 3 o la lettera C, che nelle tabelle di conversione standard danno origine sempre al numero 3, oppure risponderà con un secco no se la cifra non è presente. A questo punto capirete che **facendo 10 tentativi** con tabelle di conversione opportunamente modificate, è possibile conoscere la presenza o meno delle 10 cifre decimali all'interno del PIN. Questo è il principio che sta alla base del funzionamento degli algoritmi descritti da Bond e si esplica in dei veri e propri metodi, che noi non ci sentiamo di riportare in questa sede ma che sono naturalmente presenti nel rapporto tecnico (leggete a tal proposito le motivazioni nel box).





>> L'epilogo del caso Citibank

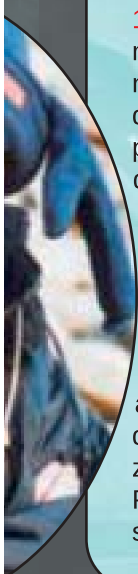
Dopo la ricerca di Mike Bond, la Citibank si è trovata un po' spiazzata e ha subito provveduto a richiedere all'Alta Corte inglese, forte di una sentenza favorevole già ottenuta in Sud Africa, che **i documenti relativi alle ricerche di Anderson e del suo studente Bond venissero bandite da qualunque mezzo di diffusione pubblica** tra cui in particolare internet, lezioni o seminari pubblici, discussioni su riviste specialistiche. Purtroppo l'Alta corte inglese ha accolto la richiesta senza che però di fatto i documenti venissero eliminati dalla rete come potete notare dai link presenti nel box.

Questa sentenza è la concretizzazione di una questione che è sempre stata cara all'-hacking e cioè: **è giusto limitare la possibilità di conoscenza e di studio dei sistemi informatici allo scopo di renderli più sicuri** (security through obscurity)? In un epoca in cui la diffusione delle informazioni non può essere arrestata dalla sentenza di una corte nazionale probabilmente **la risposta è no**. Ma anche se fosse possibile, sarebbe utile? Non sarebbe stato più opportuno imporre alla Citibank che un sistema inadeguato, risalente praticamente agli anni ottanta, venisse rivisto? L'Alta Corte non ha pensato ai cittadini inglesi che affidano i loro risparmi alla Citibank? Dal momento che i criminali sono probabilmente già a conoscenza della vulnerabilità, **chi rimarrebbe all'oscuro della questione sarebbero soltanto i cittadini frodati** che non sarebbero in



grado di dimostrare dinanzi ad una corte come il loro Pin gelosamente custodito sia stato utilizzato. Occhio non vede, portafoglio (della Citibank) non duole.

Roberto 'dec0der' Enea
enea@hackerjournal.it



Autocensura

Sulla trattazione tecnica dell'argomento di questo articolo abbiamo scelto di autocensurarci. La nostra trattazione è infatti parziale e non va molto nel dettaglio. Abbiamo infatti deciso di non riportare i tre algoritmi descritti da Mike Bond nel suo trattato. I motivi sono due ed entrambi a nostro parere validi:

1. L'intento di questo articolo non è quello di fornire uno strumento per commettere illeciti, ma di sensibilizzare e informare i nostri lettori su un rischio reale che, come avete potuto leggere dagli stralci di mail riportare nel box riguarda anche il nostro paese. Qualora vi capiti ciò che è capitato ai Singh, potrete dimostrare alla vostra banca come il furto di Pin sia possibile ed ottenere (forse) il giusto risarcimento. Nonostante questo, potrebbe essere frainteso dai più.
2. Il nostro codice penale vieta la diffusione di tecniche che possano essere utilizzate per commettere un reato senza fornire le contromisure (cosa che noi per altro facciamo sempre). Questa volta però non c'è alcuna contromisura da poter adottare se non la sostituzione dei sistemi di autenticazione dei PIN, operazione sicuramente non molto agevole ma senz'altro necessaria.

Per questi motivi preferiamo (un po' a malincuore) censurarci da soli per evitare che lo faccia qualcun'altro.

Link utili...

http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/citibank_order.pdf
Provvedimento dell'Alta Corte inglese contro la pubblica discussione delle vulnerabilità crittografiche del sistema della Diners/Citibank.

http://cryptome.org/gag/HSM_I&O_Manual_1270A513-3.pdf
Manuale d'installazione dell'HSM

http://cryptome.org/gag/HSM_Programmers_Manual_-1270A514-3.pdf
Manuale del programmatore dell'HSM

http://cryptome.org/gag/API-Attacks.pdf
"Attacchi alle API dei sistemi integrati" di Mike Bond e Ross Anderson

http://cryptome.org/gag/Attacks-on-Crypto-TS.pdf
"Attacchi ai criptoprocessori" di Mike Bond

Gli errori di VeriSign

Da qualche tempo, alcune connessioni Internet vengono impropriamente dirottate verso il motore di ricerca SiteFinder. Scopri come ristabilire il rispetto delle regole sul tuo computer!

Nell'editoriale dello scorso numero abbiamo parlato della novità introdotta da Verisign nella gestione degli errori per i domini .com e .net. In pratica, da qualche settimana, se sbagliate a digitare un indirizzo appartenente a questi domini, non riceverete più un messaggio di errore, ma verrete dirottati su un motore di ricerca (SiteFinder), dove potrete cercare le informazioni che desideravate trovare. Verisign, quindi, ha sovvertito un protocollo e delle regole comuni che Internet si è data, per dirottare una certa quantità di traffico su un proprio sito che ospita inserzioni a pagamento.
Tutto ciò non è per niente carino da parte di Verisign, per una serie di motivi. Innanzi tutto, questa azienda non ha la "proprietà" dei domini .com e .net, ma li ha ottenuti in concessione dall'Icann (l'organismo internazionale che a sua volta ha preso in carico la gestione di questi domini dal Governo USA), a patto che rispettasse gli accordi sul funzionamento di Internet definiti dalle RFC, veri testi sacri del networking globale.

>> Problemi concreti

A parte la questione di principio (non puoi distorcere a tuo vantaggio le regole comuni), questo comportamento rischia di mettere in crisi alcuni servizi e funzionalità della rete che basano il proprio funzionamento su una risposta corretta da parte dei server DNS. Per esempio, se si sbaglia a inserire l'indirizzo in un programma di traceroute, questo non restituirà un errore, ma calcolerà "la rotta" che porta a SiteFinder; i programmi antispam che verificano l'esistenza del dominio del mittente, non ricevendo un errore da parte dei DNS, lasceranno passare tonnellate di spam in più (come se già non ce ne fosse abbastanza). Per non parlare dei sistemi di diagnostica delle reti. Aspettando (e sperando) che la faccenda venga risolta in modo definitivo, magari anche grazie alla spinta di alcune cause già aperte nei tribunali americani contro Verisign, è bene quindi correre ai ripari e prendere qualche provvedimento pratico, alla nostra maniera.

>> Modificare il file hosts

Analizziamo il problema. Inseriamo un URL dei domini .com e .net, commettiamo un errore di digitazione, e veniamo dirottati su SiteFinder. Noi vogliamo ottenere due obiettivi: evitare di venire dirottati sul sito di SiteFinder, e ottenere un messaggio di errore.
Un prima possibilità è quella di modificare il file hosts del proprio computer. Si tratta di un file di testo che agisce come "dns privato", stabilendo una corrispondenza tra nomi di server e loro indirizzo IP. A seconda del sistema operativo utilizzato, il file si trova in queste posizioni:

Windows 95/98/Me
`c:\windows\hosts`

Windows NT/2000/XP Professional
`c:\winnt\system32\drivers\etc\hosts`

Windows XP Home
`c:\windows\system32\drivers\etc\hosts`

Linux/*BSD
`/etc/hosts (richiede accesso root)`

Per esempio, in una rete locale, si può inserire nel file hosts una riga che dice:

```
192.168.10.3 spippolo #server di prova
```



La pagina di SiteFinder, che da qualche tempo appare invece dell'errore previsto dalle RFC.

A questo punto, ogni volta che inseriremo in un browser o altro client Internet l'indirizzo "spippolo", invieremo una richiesta al server che si trova all'indirizzo 192.168.10.3 (la frase dopo il simbolo # è solo un commento). Il file hosts ha la precedenza sui DNS, e quindi lo si può usare anche per indirizzi che esistono realmente. Quindi, se noi inseriamo nel file hosts gli i nomi dei server usati da SiteFinder, associandoli a indirizzi inesistenti, otterremo un messaggio di errore ogni volta che verremo dirottati su SiteFinder. Si tratta quindi di aggiungere le seguenti righe:

```
0.0.0.0 sitefinder.verisign.com
0.0.0.0 sitefinder-
idn.verisign.com
```

>> Soluzione poco efficiente

Il sistema visto qui sopra però risolve solo uno dei problemi, e in modo parziale. L'interrograzione, in effetti va a buon fine: il nome viene risolto dal DNS e veniamo inviati al server di Verisign. Solo a questo punto interviene il file hosts, che non restituisce immediatamente un errore, ma cerca di contattare un server che non esiste; solo dopo un po' di tempo arriverà un errore di time-out nel tentativo di collegarsi al server (o di connessione rifiutata, a seconda dei casi), che non è l'errore che ci si aspetta. Inoltre, il tutto potrebbe richiedere un po' di tempo. Se si cerca di accelerare il processo, per esempio inserendo 127.0.0.1 (cioè l'indirizzo del proprio computer) o un altro indirizzo valido (per esempio la propria home page, o google.com), otteniamo sì il risultato di non venire inviati al server di SiteFinder, ma veniamo comunque inviati a un indirizzo valido, e si vanifica uno degli obiettivi.

>> Bloccare alla fonte

È necessario quindi trovare un altro metodo più rapido e più efficace, che blocchi il collegamento prima ancora che venga effettuata la richiesta di collegamento al server di Verisign. Questo è il lavoro per un firewall!
Prendiamo quindi gli indirizzi annotati sopra, e creiamo delle regole per il nostro firewall che impediscano qualsiasi collegamento ai server di Verisign corrispondenti al servizio SiteFinder. La procedura è diversa a seconda del firewall utilizzato, ma la sostanza della regola dovrà essere:

```
Nega qualsiasi collegamento
TCP che ha come destinazio-
ne i server
sitefinder.verisign.com e
sitefinder-idn.verisign.com
```

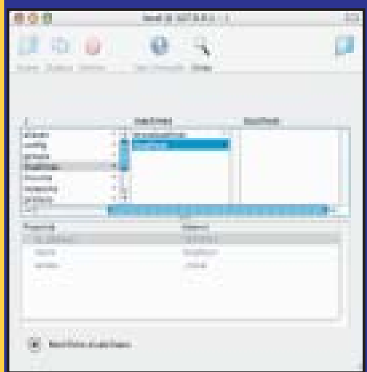
Su Linux, si può usare iptables, che è il firewall predefinito su molte installazioni. Con il seguente comando, per esempio, si aggiunge una regola che dice a iptables di respingere le richieste indirizzate all'indirizzo 64.94.110.11 (quello di SiteFinder), con un messaggio che dice che l'host è irraggiungibile.

```
iptables -A blocked_sites -
p TCP -d 64.94.110.11 -j
REJECT –reject-with icmp-
host-unreachable
```

>> Meno pratica, ma più efficace

A parte questi espedienti personali (che ci sono utili anche per capire qualcosa di più di come funziona il nostro computer), quello provocato da SiteFinder è un problema dell'intera rete, e che va affrontato a livello di rete e di comunità. E la comunità si è già attivata: gli sviluppatori di molti software per server DNS, primo tra tutti il diffusissimo Bind, hanno già rilasciato della patch per i loro programmi, che aggirano il problema in modo pulito e trasparente per l'utente. Il problema è che questi software devono essere installati e configurati dal provider, e al momento non sono molti quelli che - almeno in Italia - hanno provveduto a effettuare la modifica.
Una cosa che potete fare quindi è scrivere al supporto tecnico del provider per richiedere che i server DNS vengano aggiornati alla versione più recente. Del resto, il fatto che un server risponda come ci si aspetta che faccia, è un vostro pieno diritto.

Con i computer della mela...



Mac OS X ha un file hosts, ma viene interpellato soltanto in alcuni casi. Le modifiche ai nomi dei server vanno invece apportate attraverso l'applicazione Gestione NetInfo (NetInfo Manager), presente nella cartella Applicazioni/Utility. Attraverso Gestione NetInfo, un utente inesperto può fare danni raccapriccianti al Sistema, per cui evitiamo direttamente di spiegare come fare (chi ha le conoscenze, può trovare le informazioni su Internet).
Per quanto riguarda invece il metodo che prevede l'uso di un firewall, se non si utilizzano applicazioni dedicate, ci si può appoggiare all'efficace firewall di sistema. Questo va attivato attraverso il pannello Condivisione di Preferenze di Sistema. Per aggiungere le regole che bloccano i server di Verisign, bisogna impartire i seguenti comandi da terminale:

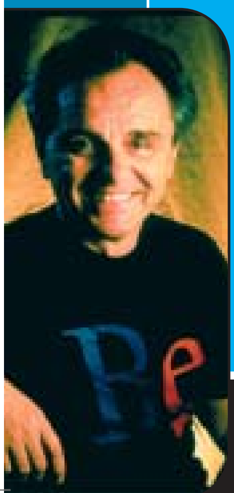
```
sudo ipfw add 1170 deny tcp from any to sitefinder.verisign.com
sudo ipfw add 1170 deny tcp from any to sitefinder-idn.verisign.com
```

Le modifiche alle regole di ipfw devono essere eseguite coi privilegi di amministratore (attraverso sudo), per cui dopo il primo comando, bisognerà inserire la password.

BeOS – Be different

Un sistema operativo dalle spiccate caratteristiche multimediali, che pu rappresentare un'alternativa a Windows, e anche a Linux.

Pensate ad un sistema operativo progettato per supportare e sfruttare più processori contemporaneamente, basato su un microkernel, un 'cuore' piccolo e modulare, rapido e reattivo anche su sistemi poco potenti ma allo stesso tempo dotato di multitasking e memoria protetta. A questo aggiungete un filesystem a 64 bit che permette di avere file più grandi di un Terabyte, che offre una funzione di 'journaling' e che supporta molti filesystem di altri OS, che pur non essendo uno UNIX ha una shell di tipo 'bash' e l'aderenza allo standard POSIX ma allo stesso tempo l'implementazione di OpenGL, una predisposizione al video ed all'audio con midi integrato. Infine aggiungete un'interfaccia chiara, essenziale ed elegante, e un design ad oggetti che ottimizza la programmazione, l'ottimizzazione delle risorse e il riutilizzo delle stesse. Quello appena descritto **è un sistema che esiste sin dalla seconda metà degli anni '90**, dal 1995 per la precisione, e che risponde al nome di **BeOS**.



>> Cos'è BeOS? Qual'è la sua storia?

BeOS è un sistema operativo che non deriva da nessun altro sistema preesistente; è scritto da zero e implementa soluzioni e caratteristiche moderne, ma non sbuca dal nulla. È frutto di **un team capitanato da Jean Luis Gassee**, carismatico ex-dirigente Apple.

Gassee è tra le altre cose anche il fondatore della filiale europea della casa di Cupertino e alla Apple ha svolto, fino al 1990, un ruolo di primissimo piano nella progettazione e direzione tecnologica (qualcuno dice anche troppo, addebitandogli in parte l'attuale posizione di nicchia del Mac, a causa di una condotta troppo elitaria e poco propensa a compromessi ed accordi).

Lo stesso anno, Gassee, insieme al collega Steve Sakoman che ha un passato in Silicon Graphics, HP ed Apple (e altri provenienti da Adobe, Opcode, Microsoft) fonda la Be, Inc. che inizialmente punta su **un'accoppiata di hardware proprietario** (una macchina multiprocessore PowerPC, la BeBox) **+ BeOS**, che viene implementato anche per i sistemi Macintosh.

L'idea dietro il progetto era quella di costruire una macchina che rappresentasse una soluzione innovativa per la gestione dei dati multimediali, e che suscitasse lo stesso senso di lealtà e attaccamento del computer Amiga, computer che aveva affascinato per anni Gassee.





In realta la BeBox, presentata dopo cinque anni, seppur con prezzo e caratteristiche interessanti quali l'enorme numero di connettori e interfacce a disposizione (http://www.bebox.nu/images/bebox/ppc/bebox-back-large.gif) **non prese mai il volo e all'inizio del 97 fu abbandonata**.

La Be si concentrò quindi sul BeOS, rilasciando lo stesso anno la versione 2 per piattaforme Apple e cloni.

>> Be ed Apple: un accordo mancato

Nel frattempo, il BeOS **per un pelo non divenne la base del nuovo OS di Apple**: la spuntò un altro fuoriuscito, il cofondatore Steve Jobs, con il

NEWBIE

Be Amarcord



Per chi fosse incuriosito dalla storia e dal folklore dietro alla Be e ai suoi prodotti, in rete sono disponibili numerosi siti web con informazioni e iconografia. Tra tutte vi segnaliamo due gallerie di immagini presenti sul sito ww.bebox.nu

La prima è dedicata a Joe Palmer, progettista del BeBox e del computer speciale di cui gli è stato fatto dono prima di lasciare la ditta, firmato e istoriato con scritte e dediche da tutti gli impiegati della Be, Inc.

http://www.bebox.nu/images.php?s=images/joepalmer

La seconda è una cronistoria delle varie versioni del BeOS, con foto di scatole, dischetti e CD, tra cui anche numerose beta e copie interne.

http://www.bebox.nu/images.php?s=images/beosversions



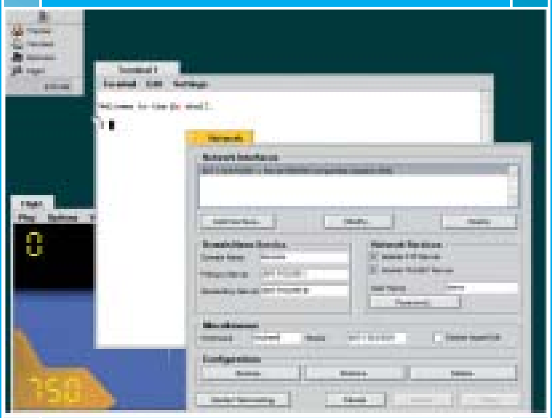
suo NeXT, anch'esso innovativo e 'object oriented'. Anche per questo motivo, le relazioni con la casa della mela deteriorano rapidamente e la Be decise di **iniziare il porting anche per i PC (x86)**, reso realtà nel 1998. Nel giro di due anni si sono susseguite varie versioni arrivando alla R5 nel marzo 2000, che fu diffusa in forma limitata (il nome esatto era 'Personal Edition') in forma gratuita per PC e che rappresenta sia il punto di massima diffusione che l'ultima versione ufficiale rilasciata.

In realtà il rilascio della versione gratuita del BeOS (ne esiste tuttora in rete una scaricabile e usabile liberamente) ha numerosi retroscena: tra questi c'è la **difficoltà nel fornire il sistema operativo a distributori OEM per via degli ostacoli creati da Microsoft con i suoi discutibili contratti** (che ha portato ad una lunga procedura di causa risoltasi solo quest'anno a favore di ciò che rimane della Be, Inc.) e l'obiettivo di rendere più semplice provare il sistema senza dover ripartizionare il disco rigido per installarlo.

Purtroppo, la 'Personal Edition' da un lato faceva crescere la popolarità, ma dall'altro danneggiava anche le vendite della versione 'completa' (commerciale): la fine si approssimava perché la Be Inc. aveva accumulando **debiti per oltre 54 milioni di dollari**. L'ultimo tentativo di ripresa, e probabilmente anche l'errore finale, fu la decisione di riciclare le attività e gli sforzi nella creazione di **una versione particolare dell'OS, BeIA , "Be [for] Internet Appliance[s]" (Be [per] i Dispositivi Internet)**, che ebbe solo il risultato di arrestare lo sviluppo software di terze parti per il BeOS. È a questo punto che inizia l'interessamento della Palm.

>> Palm compra le proprietà Be

È dell'agosto 2001 l'annuncio ufficiale che la Palm aveva acquisito il patrimonio intellettuale, in pratica **tutto il know-how e le tecnologie della**



Be per la cifra di 11 milioni dollari statunitensi. Le motivazioni della Palm parlano di interesse a potenziare la connettività e il lato multimediale dei suoi prodotti, cosa poi confermata dai fatti quando circa due anni dopo con la versione 6.0 del sistema operativo PalmOS che incorpora **alcuni algoritmi ed architetture della ditta di Gassee**.

La reazione immediata degli utenti è di



preoccupazione, sopratutto perché le dichiarazioni della Palm erano chiarissime e specificavano che **non c'era alcuna intenzione di proseguire lo sviluppo del BeOS** né tantomeno di accettare la proposta economica (www.kuro5hin.org/story/2001/4/19/153837/408) di un gruppo di sviluppatori di rilevare e proseguire lo sviluppo dell'OS.

La risposta a questa situazione è stata la nascita di una pletora di progetti dai metodi, dalle caratteristiche e dalle specifiche spesso anche molto diverse tra di loro. L'obiettivo dei vari **BlueEyedOS**, **Atheos**, **Leonardo**, **Cosmos**, **OSBOS** era lo stesso: creare un nuovo sistema operativo che incarnasse lo spirito e la filosofia del BeOS, anche grazie alla disponibilità di alcune parti del sistema che la Be Inc. aveva reso pubbliche. A coordinare i progetti (ed a tenerne traccia) c'è un sito indipendente e no-profit, BeUnited (www.beunited.org).

A questa situazione, molto fluida sino ad oggi, si aggiunge **una versione illegale ed ancora sperimentale del BeOS**, la 5.1 (chiamata "Dano"), diffusa probabilmente da qualche dipendente della Be. Questa versione, a tutti gli effetti una copia intermedia tra la 5 e la 6 contiene numerose chicche e migliorie tra cui una nuova gestione del networking, l'accelerazione della grafica OpenGL e una nuova interfaccia grafica, aumentando sia la sensazione generale di "diaspora" che la frustrazione di ciò che sarebbe potuto diventare in futuro il BeOS.

>> La situazione attuale

Vediamo ora una panoramica sulle varie iniziative che vogliono raccogliere il testimone, ottimamente presentate oltre che sul già citato BeUnited anche sul sito dell'itBUG (www.itbug.org), l'agguerrito 'User Group' italiano di BeOS.

BlueEyedOS (www.blueeyedos.com), **BeFree** (befree.berlios.de/) e **Cosmoe** (www.cosmoe.com) intendono ricreare il BeOS sposandolo con (o sovrapponendolo a) una solida base costituita perlopiù da Linux o BSD.

OpenBeos (www.openbeos.net) inve-

Libro free per sviluppatori



Uno dei primi accordi stipulati dalla nascitura Be Inc nella metà degli anni '90 è stato quello con la O'Reilly. La nota casa editrice di manuali tecnici dall'eccellente fattura è stata la fonte di riferimento per la ditta di Gassee, pubblicando nel 1999 un libro a firma di Dan Parks Sydow, "Programming the Be Operating System", che documenta ed assiste gli sviluppatori a scrivere applicazioni per il BeOS. Nell'estate del 2003 questo libro, come già successo per altri volumi, ormai esaurito e fuori catalogo è stato reso liberamente scaricabile dalla O'Reilly.
All'indirizzo www.oreilly.com/catalog/beosprog è perciò possibile scaricare in pdf tutte e 397 le pagine del libro, un'interessante manuale per il programmatore o il curioso che vuole avvicinarsi e capire la tecnologia alla base del BeOS.



ce vuole ricreare totalmente il BeOS ed è attualmente il progetto giunto ad uno stadio più avanzato, prossimo ad una presentazione ufficiale.

Nel panorama costituito da questi progetti "free" o comunque "aperti" ha fatto capolino e si è ritagliata sempre più spazio, inizialmente tra molte critiche e



dubbi, **una proposta commerciale: Zeta**. Sviluppata dalla tedesca **YellowTab** (www.yellowtab.de) è a tutti gli effetti la prosecuzione commerciale autorizzata e legale di BeOS in quanto, è stato svelato, **aveva preso accordi di licenza in tal senso con la BeOS** quando questa si era concentrata su BeIA.
Zeta, il cui nome sta per "vita" ed è tratto da un film (http://iltuosistema.altervista.org/articolo25.html), è ormai prossima ad una release ufficiale e sarà disponibile in tre versioni dai nomi autoesplicativi: la "**Home Edition**" (dal costo di 49 dollari), la "**Deluxe Edition**" (su DVD, 99 dollari) e la "**Developer Edition**" (69 dollari).
C'è chi cita il BeOS e le idee alla sua base come uno delle ultime grandi innovazioni in campo di sistemi operativi, ed effettivamente un sistema giovane e pensato con coerenza ed attenzione all'interfaccia come alla reattività non può che essere benvenuto in un decennio fin troppo appiattito sull'omologazione informatica generale.

Una cosa è certa: la voglia di far rinascere il BeOS e rafforzare uno dei più interessanti sistemi operativi è molta e numerose sono le forze all'opera. Non rimane che aspettare il rilascio di qualcuno degli eredi, commerciale o 'free' che sia.

Nicola D'Agostino
dagostino@nezmar.com

Si ringrazia Giuseppe Gargaro e Christian Celona dell'ItBug (http://www.itbug.org), il gruppo degli utenti italiani di BeOS.

Beyond, una rivista italiana in Pdf



Il già citato itBUG (Italian BeOS User Group) ha di recente sfornato una interessantissima rivista in pdf chiamata Beyond, che parla con articoli e news di sistemi operativi 'alternativi' quali Amiga, MacOS X, Linux, FreeBSD e naturalmente BeOS.
Il primo numero è datato agosto 2003 e dietro una grafica ed impaginazione professionali (chissà che non possa venire stampato in allegato a qualche rivista...) parla di MSX e emulazione, di programmazione e connettività ADSL per BeOS, offre un reportage dal tour promozionale Amiga Alpe Adria 2003 e fa una disamina dei filesystem di BeOS e di OSX.
Beyond è disponibile all'url beyond.itbug.org ed è disponibile sia in versione italiana che in inglese.

HACKER JOURNAL

Anno 2 - N. 35
9 Ottobre - 23 Ottobre 2003

Boss: theguilty@hackerjournal.it
Editor: grand@hackerjournal.it
Contributors: Bismark.it, DaMe`, Nicola D'Agostino, Roberto "decOder" Enea, S.O.S. - Korn, >>--Robin-->, Roberto Valloggia
DTP: Cesare Salgaro
Graphic designer: Dopla Graphic S.r.l. info@dopla.com
Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. a Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile - Editore Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack'er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

BREVETTI SUL SOFTWARE:

VINTA UNA BATTAGLIA, MA LA GUERRA CONTINUA

La normativa europea sui brevetti è stata approvata, ma con modifiche sostanziali rispetto al testo proposto su "ispirazione" della BSA, l'associazione che raccoglie le principali software house mondiali. Come spesso accade dopo le elezioni, ogni parte politica in causa dichiara di aver ottenuto una importante vittoria. Possibile? Ma è proprio vero? Facciamo un passo indietro per capire innanzi tutto qual è l'oggetto del contendere.

Attualmente, in Europa la proprietà intellettuale sul software è coperta dalla legge sul diritto d'autore, e non dai brevetti. Il software è quindi paragonato più a un'opera letteraria o musicale che a un'invenzione. Non si possono brevettare le idee, ma solo la loro realizzazione pratica (le invenzioni, appunto). Anche su questo ci sarebbe da discutere, ma prendiamolo come dato di fatto. La legge votata il 22 settembre voleva appunto modificare questo stato di cose, permettendo la brevettabilità di algoritmi, porzioni di codice e semplici idee.

Su questo punto, la pressione esercitata sul parlamento europeo dalla mobilitazione di migliaia di cittadini (ma anche, bisogna dirlo, di decine di scienziati e rappresentanti di federazioni commerciali e industriali), sembra aver raggiunto i suoi scopi: per ora, il Parlamento Europeo ha stabilito che i brevetti non si possono applicare al software né alle idee.

Già, per ora, perché un testo approvato dal Parlamento Europeo non diventa automaticamente una legge valida in tutto il Vecchio Continente. La decisione finale spetta infatti alla Commissione, che non è eletta dai cittadini ma nominata dai governi. La commissione "dovrebbe" rispettare il volere del Parlamento, nel ratificare le sue direttive, ma non è tenuta a farlo alla lettera. In più, ogni Parlamento nazionale dovrà approvare leggi che rispettino le direttive della Commissione.

Anche il parziale successo ottenuto quindi al Parlamento Europeo (parziale perché, comunque, non tutti i punti contestati sono stati esclusi dal testo finale), rischia di essere una vittoria di Pirro.

Però da tutto questo abbiamo imparato qualcosa: se stiamo attenti a ciò che succede nel mondo della politica, possiamo accorgerci in tempo quando i potenti cercano di cancellare un diritto, o di sottrarci delle libertà. E una volta scoperti, possiamo fare abbastanza rumore da farci sentire, e condizionare le loro scelte.

La prima parziale vittoria deve quindi servire come stimolo a tenere alta la guardia, e sorvegliare tutti i prossimi appuntamenti nel corso dell'iter di queste leggi, a ogni livello. Noi non molleremo: saremo sempre qui, a tenervi informati su ciò che succede. Senza vincoli né peli sulla lingua.

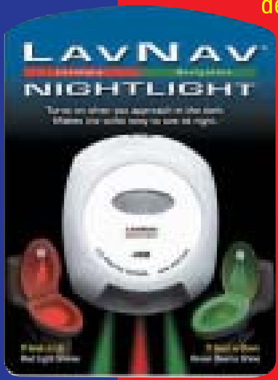
grand@hackerjournal.it

NEWS

HOT!

MAI PIÙ FUORI DAL BUCO

Chi non ha rischiato almeno una volta di sbagliar mira mentre si apprestava a fare ehm, certi scroscianti bisogni nel cuore della notte? Una ditta californiana che ha preso molto seriamente tale inconveniente, ha pensato a una brillante soluzione. Inventare un marchingegno che, tramite un sensore installato alla base del WC, rileva il nostro avvicinamento e accende una luce sulla tazza. Rossa se la tavoletta è sollevata, un avvertimento per il genti sesso. Verde se è abbassata, un avvertimento per i signori maschietti che faranno bene ad alzarla prima di liberarsi, onde evitare successive estenuanti discussioni sull'argomento con le donne di casa. Questa furbata permetterà inoltre di raggiungere l'anelato luogo senza accendere altre luci, dunque senza rischiare che familiari disturbati nel sonno e imbufaliti ci tirino ciabatte e quant'altro. L'oggetto si chiama LavNav e costa solo 30 dollari.



ADDIO COCCINELLE

Altro che le coccinelle e ammennicoli vari a calamita che fino a qualche tempo fa andavano di moda per difenderci dai campi elettromagnetici generati dai cellulari. Roba superata. Negli Stati Uniti stanno mettendo a punto un orologio che funziona da schermo totale contro l'inquinamento elettromagnetico di telefonini, computer e simili. Un chip interno genera frequenze che vanno a neutralizzare quelle dannose per la nostra salute. Funzionare funziona. Parola di chi lo ha provato: meno stanchezza, niente mal di testa, migliori prestazioni. E se anche non funzionasse, poco male: ha un look così trendy, che non rimpiangeremmo la somma sborsata.



IL GRANDE GENITORE

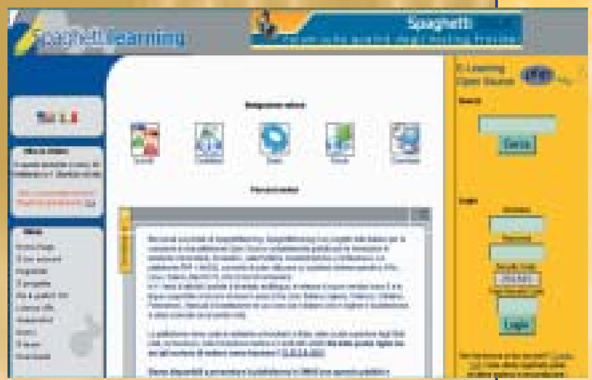


Altro che Grande Fratello! Il lungo braccio del controllo di mamma e papà si avvia a divenire un mostro tentacolare. Tutto per colpa della tecnologia.

I cellulari ci rendono sempre raggiungibili, le pagelle elettroniche e il registro delle assenze online non ci permettono più di farla franca. E ora dagli Stati Uniti sta arrivando la RS-1000 Black Box, una specie di scatola nera da mettere sull'auto che registra tutte le malefatte automobilistiche, per fortuna solo quelle, dei figli sciagurati. Verranno memorizzate infrazioni dei limiti di velocità, mancato allacciamento delle cinture, curve troppo brusche. Ci sarà persino un resoconto della strada percorsa. Che significa che ogni volta che invece che in biblioteca a studiare, andremo a svaccarci al parco o a infrattarci con la fidanza, mammà lo verrà a sapere. Una pestilenza. Ma non è finita. Per riportare alla disciplina guidatori troppo sportivi la Black Box dispone di un segnalatore acustico che avverte dell'infrazione. Inutile cercare di mettere a chiodo l'autoradio: il volume del gendarme elettronico si alzerà di conseguenza. È la fine. Ma giacchè si dice che "a mali estremi, estremi rimedi", quanti giorni dovranno passare prima che la scatola nera venga hackerata? Si accettano scommesse.

SPAGHETTI PER L'ISTRUZIONE

Piatto goloso sul tavolo dell'insegnamento a distanza. Realizzata da Spaghetti Learning, gruppo di lavoro completamente italiano, è da poco disponibile una piattaforma per e-learning Open Source gratuita. La piattaforma è l'ideale per gestire progetti di formazione a distanza in tutti gli ambiti: lavorativo, scolastico, universitario e della pubblica amministrazione. Le principali funzionalità della piattaforma sono: impostazioni e monitoraggio dell'attività utente; supporto lezioni anche multimediali; test; interazione docente-allievo basato su chat e forum. Chi fosse interessato troverà tutte le informazioni necessarie sul sito all'indirizzo www.spaghettilearning.com Per avere un'idea concreta del prodotto e delle sue applicazioni dalla home del sito è possibile scaricare una demo.



PROIBITO CONDIVIDERE

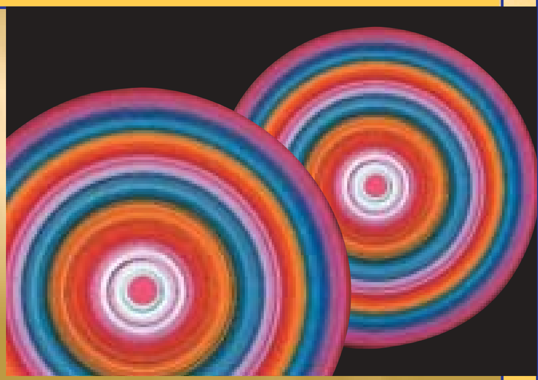
Anche se non siamo fan dell'artista soul Anthony Hamilton, l'uscita del suo ultimo disco lo scorso 23 settembre, dovrebbe averci fatto alzare le antenne. Motivo? Le nuove protezioni prodotte da SunnComm e inserite nell'album dalla casa discografica Arista Records, divisione di BMG. Il sistema di protezione adottato è piuttosto diverso dai precedenti. E soprattutto ha l'aria di voler dare un contentino al pubblico, cercando di ingraziarselo con qualche concessione in più. Il cd contiene infatti file in mp3 da scaricare sul computer, che però sono codificati in maniera tale da impedire alcune operazioni tra cui la condivisione.



In compenso, chi acquista il CD potrà masterizzare tre copie delle canzoni. Il disco fornirà inoltre un collegamento di condivisione che permette lo scaricamento dell'album da parte di altre persone e il suo ascolto per soli dieci giorni.

NUOVI CD STESSA FREGATURA

Le case discografiche non si rassegnano. Soprattutto fanno finta di non capire che le vendite dei CD forse sono crollate perché ormai per comprane uno bisogna chiedere un fido alla banca. Allora per aggirare il problema cosa fanno? Ne pensano di tutti i colori. L'ultima trovata di Warner e Sony è il dual disc, un nuovo supporto che da un lato, su cd, contiene le tracce audio dall'altro, su dvd, i video degli artisti. Naturalmente il dual disc costerà come prima o più di prima. Dunque cosa si risolverà? Niente. Meditate signori discografici, meditate.



FINALMENTE UN WORM BUONO



Niente a che vedere con i virus informatici. Il worm di cui parliamo lo hanno inventato a Tokyo, si chiama Koga ed è un vermiciattolone telecomandato che, portato sul teatro dei terremoti, aiuterà i soccorritori a individuare persone ancora in vita sotto le macerie. Koga ha una telecamera montata sulla testa e si sposta in maniera appositamente studiata per non generare crolli. L'unica pecca del bruco da soccorso è la resistenza. Le batterie durano infatti solo 30 minuti.
Koga non è unico nel suo genere, ha anche una "cugina": Moira, un prototipo analogo lungo quasi un metro e mezzo, realizzato dall'Università di Kyoto.

DIALER? NO GRAZIE!

Annebbiati dai fumi del coinvolgimento dei giochi online, anche ai più sgamati almeno una volta può succedere di cadere nella trappola dei dialer. Col risultato di vedersi recapitare bollette telefoniche che stenderebbero anche un bisonte. Per giocare online senza lo stress di ricevere fregature, adesso c'è un portale sicuro. Si chiama Giochi.org e lo troviamo all'indirizzo internet www.giochi.org. I giochi sono tutti in flash, commentati in italiano e divisi per categorie. Presto verrà inaugurata una sezione di giochi multiplayer e una di giochi da usare con telefonini e palmari.

LAUREA IN SICUREZZA INFORMATICA

Da quest'anno chi ha sempre avuto il pallino della sicurezza informatica potrà trasformare la sua passione in un bel certificato di laurea. Bastano tre anni di corso presso il polo universitario Cremasco dell'Università di Milano, ed eccoci togati Dottori in Sicurezza dei sistemi e delle Reti informatiche. Le materie di studio sono molto varie, alcune strettamente tecnico-pratiche, altre di più ampio respiro. Algoritmi e strutture dati, crittografia, diritto dell'informatica, finanzia aziendale solo per citarne alcune tra le tante. Di sicuro il corso di laurea garantirà buoni sbocchi professionali. Con i tempi che corrono un buon esperto di informatica, di reti di computer e di lotta alle i intrusioni nei sistemi informatici, non tarderà a trovare lavoro. Per avere maggiori informazioni e per consultare il piano di studi colleghiamoci al sito della facoltà: http://www.dti.unimi.it/corso.php?z=0;id_corso=7

HOT!

A SCUOLA DI LINUX



Autunno è tempo di corsi di ogni genere. Perché non cimentarsi in un corso di Linux. Ne abbiamo scovati alcuni completamente gratuiti, uno dei quali finanziato da Unione Europea, Fondo sociale Europeo, Ministero del Lavoro e Regione Lombardia. Il corso è destinato a 12 diplomati, in cerca di prima occupazione, iscritti alle liste di mobilità o studenti. Tra gli argomenti affrontati nelle lezioni: visione di insieme del sistema operativo, configurazione della rete, installazione e aggiornamento del software, utilizzo dei principali servizi, analisi del boot dei processi e della rete e molto altro ancora. Al termine del corso ai partecipanti verrà rilasciato il certificato di qualifica di secondo livello.
Per ulteriori informazioni: sistema imprese sociali-settore formazione: e-mail segformazione@consorziosis.org
Tel. 02.2688.011



LINUX, L'ALTERNATIVA INFORMATICA

L'iscrizione è aperta indifferentemente ai soggetti occupati e in cerca di occupazione. Il corso è finanziato dal Fondo Sociale Europeo ed è completamente gratuito.
Luogo del corso: Pordenone
http://www.ialweb.it/shownews.asp?idnews=634

TECNICO DI SISTEMA E NETWORKING LINUX

Luogo del corso: Milano
http://www.formazionein.it/site/dettaglio_corso.asp?id_formazione=366

SISTEMISTA IN AMBIENTE LINUX

Luogo del corso: Legnano
http://www.campusnet.it/corsi2003_2004.asp